

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

**INFORMATION TECHNOLOGY (IT) ETHICS: TRAINING
AND AWARENESS MATERIALS FOR THE
DEPARTMENT OF THE NAVY**

by

Jasper W. Senter III

September 2002

Cayetano S. Thornton

June 2002

Thesis Advisor:

Cynthia E. Irvine

Associate Advisor:

Floyd Brock

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June/September 2002	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Information Technology (IT) Ethics: Training and Awareness Materials for the Department of the Navy			5. FUNDING NUMBERS	
6. AUTHOR(S) Jasper W. Senter III, (September 2002) and Cayetano S. Thornton, (June 2002)				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE	
<p>ABSTRACT (maximum 200 words) Information ethics is a relatively new field of study that aims to identify and to analyze the impact technology has on society, personal values, and the application of ethics in cyberspace. The Department of the Navy (DoN) continues to experience incidents of unethical behavior by personnel using government computers and accessing the Internet from within government networks. These incidents will continue and grow in number as the Navy and Marine Corps' dependence upon information technology (IT) increases. There are circumstances requiring ethical decision making encountered by naval personnel that are not sufficiently addressed by policy. Many of these situations do not neatly translate from ordinary experience to the IT world. These topics include the right to privacy, the protection of intellectual property, the collection and stewardship of information, and cyber crime. To address this problem, training materials on a CD-ROM have been created with the objective of giving DoN personnel a better understanding of the ethical responsibilities that are required when using IT. The training materials provide decision making tools to better prepare naval personnel when facing ethical dilemmas in the IT context.</p>				
14. SUBJECT TERMS Ethics; Information Technology; Networks; Training; Awareness			15. NUMBER OF PAGES 81	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**INFORMATION TECHNOLOGY (IT) ETHICS: TRAINING AND AWARENESS
MATERIALS FOR THE DEPARTMENT OF THE NAVY**

Jasper W. Senter III
Major, United States Marine Corps
B.B.A., University of Oklahoma, 1990
September 2002

and

Cayetano S. Thornton
Lieutenant, United States Navy
B.S. Southern Illinois University, 1996
M.A., Webster University, 2001
June 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL

Author: Jasper W. Senter III

Cayetano S. Thornton

Approved by: Cynthia E. Irvine, Thesis Advisor

Floyd Brock, Co-Advisor

Deborah Shifflett, Co-Advisor

Dan C. Boger, Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information ethics is a relatively new field of study that aims to identify and to analyze the impact technology has on society, personal values, and the application of ethics in cyberspace. The Department of the Navy (DoN) continues to experience incidents of unethical behavior by personnel using government computers and accessing the Internet from within government networks. These incidents will continue and grow in number as the Navy and Marine Corps' dependence upon information technology (IT) increases. There are circumstances requiring ethical decision making encountered by naval personnel that are not sufficiently addressed by policy. Many of these situations do not neatly translate from ordinary experience to the IT world. These topics include the right to privacy, the protection of intellectual property, the collection and stewardship of information, and cyber crime. To address this problem, training materials on a CD-ROM have been created with the objective of giving DoN personnel a better understanding of the ethical responsibilities that are required when using IT. The training materials provide decision making tools to better prepare naval personnel when facing ethical dilemmas in the IT context.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	ETHICAL FRAMEWORK.....	3
A.	ETHICS MODELS	3
1.	The Golden Rule.....	3
2.	Utilitarianism.....	4
3.	Pluralism	5
B.	ETHICS AND TECHNOLOGY	6
C.	MILITARY APPLICATION.....	8
III.	THE CONTEXT OF INFORMATION ETHICS	13
A.	A SOCIETY OF TECHNOLOGY	13
1.	Right to Privacy, Workplace Surveillance, and Appropriate Use.....	14
2.	Respect for Intellectual Property.....	19
3.	Collection, Stewardship, and Use of Information	21
4.	Cyber Crime	24
B.	TAXONOMY OF BEHAVIOR	26
1.	Typical DoN Users.....	28
2.	DoN IT Professionals	29
3.	The Role of Naval Leadership.....	30
IV.	TRAINING AND AWARENESS	33
A.	TRAINING MATERIAL	33
1.	iTechs Training CD.....	33
a.	CD Layout.....	34
b.	Training Methodology.....	34
c.	Importance of Lecture/Discussion Format.....	35
2.	Decision Making.....	35
B.	AWARENESS MATERIAL.....	37
V.	CONCLUSION.....	39
	APPENDIX A	43
	APPENDIX B.....	53
	LIST OF REFERENCES	59
	INITIAL DISTRIBUTION LIST	63

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Activity and behavior.....	26
Figure 2.	iTechs Training Flow Map.....	34
Figure 3.	iTechs Introduction Page.....	43
Figure 4.	iTechs Purpose and Objectives Page.....	44
Figure 5.	iTechs What is IT Ethics Page	45
Figure 6.	iTechs Ethics and Technology Page.....	46
Figure 7.	iTechs Organizational Viewpoint Page.....	47
Figure 8.	iTechs Decision Making Page.....	48
Figure 9.	iTechs Toolbox Page.....	49
Figure 10.	iTechs MP3 Download Scenario Page.....	50
Figure 11.	iTechs On-line Bill-pay Scenario Page	51
Figure 12.	iTechs Decision Making Awareness Poster	54
Figure 13.	iTechs Decision Steps	55
Figure 14.	iTechs 10 Commandments	56
Figure 15.	iTechs Screen Saver/Wallpaper	57

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Terminology Comparison	7
Table 2.	Taxonomy of “Gray Area” Behavior	27

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to acknowledge and thank the following people:

1. Our parents, for the support they have always shown us through the years.
2. Our wives, for enduring the many evenings away from home to conduct research for the completion of this thesis.
3. To our children, who love us even when we couldn't make it to all their activities.
4. To the Personnel Support Detachment at Naval Postgraduate School for their willingness to help in the photos taken for the scenarios.
5. The incredibly talented Matthew Rose, for the work conducted on the thesis and the creativity poured into the CD-ROM. We also appreciate the many occasions of levity he provided through this whole process.
6. Deborah Shifflett, for her patience and behind the scenes work.
7. Professor Floyd Brock, for his perspective, insight, advice, and desire to "get it done."
8. Professor Cynthia Irvine, for her painstaking attention to detail, her patience, and her expertise in a collaboration of this sort. Our many late days completing this thesis were matched by her nights and weekends ensuring that our work was thorough, relevant, and focused on the problem we wanted to solve.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The networked environment we live in today has resulted in changes to the way we work, communicate, interact with others, and generally view the world. The accelerated timing of technological developments has created a gap between those on the cutting edge and those being left behind. Currently only 54 percent of people in the United States have access to the Internet. [Ref. 1] This statistic illustrates that dependence upon technology is not universal. However, within today's military, not only is technological dependence universal, but it is paramount to day-to-day operation. This dependence upon information technology brings other issues to the forefront such as security, cost and life cycle management, and proper usage. The proper use of technology is an issue that has been inadequately addressed and needs attention.

The Navy and Marine Corps have experienced a number of incidents of unethical behavior by personnel while using government computers and networks and while accessing the Internet from within government networks. The military Honor Code mandates that military personnel be held to a higher standard of behavior than that typically expected of civilians. When personnel fail to meet this standard, the repercussions can be damaging. Concurrently, in today's military, personnel have more autonomy which requires them to exercise personal judgment and decision making more than ever before.

History has shown that ethical issues tend to follow advances in technology. From this, we may surmise that as our dependence on information technology increases so will the ethical issues we face as an organization. Deborah Johnson, a prominent author in the field of information ethics, notes "Technology instruments human action and technology makes it possible for individuals and institutions to behave in ways they couldn't behave without technology." [Ref. 2] This new relationship between humans and technology creates gray areas regarding authorized or acceptable use and unauthorized or illegal use which are not defined under our traditional ethical norms. These gray areas often go undefined, unmonitored, or unnoticed. The behavioral

standards of honor, courage, and commitment should be used to help individuals stay within the guidelines provided by the Department of Defense (DoD).

The purpose of this study is to discuss the differing philosophical viewpoints of ethics and how they apply to the realm of Information Technology (IT). In addition, this study will identify and differentiate between acceptable and unacceptable behavior. Based on the study, we have created CD-ROM-based training materials to aid in the training and awareness of system administrators, desktop users, and leaders in the appropriate use of IT within the context of the execution of military duties. To achieve a high level of ethical behavior within an organization, leadership and informed individual decision making are required. The tools discussed in this work will help to better equip government computer users with an appreciation of how the misuse of computing assets is detrimental to themselves as well as the organization.

In Chapter Two, we provide an ethical framework by discussing three ethical models and the issues that tie ethics and technology together. In the final section of this chapter, we present a military perspective of these issues as they apply to the DoN. In Chapter Three, we provide the context of information ethics by providing examples of how technology affects many aspects of society. The chapter concludes with a taxonomy of “gray area” behaviors applicable to DoN personnel. In Chapter Four, the iTechs training CD, the training methodology, and decision making are addressed. The final section contains pertinent information on awareness materials that will be used at the local command level. The conclusion provides a final overview and context for further research on this topic.

II. ETHICAL FRAMEWORK

Before addressing specific issues that are faced by sailors and Marines each day, let us provide a foundation upon which to build. First, this chapter will outline various ethical models and examples. Next, ethics and technology will be discussed together to better describe how IT creates new ethical dilemmas for society. Finally, we discuss the military aspect of ethics and technology and the imperative of training and education when it comes to the proper use of government technology resources.

A. ETHICS MODELS

For centuries experts specializing in the disciplines of philosophy and theology have tried to understand moral obligation and ethical conduct and to define the driving factors of the human decision making process. An individual's perspective toward ethics, values, and morals depends greatly upon his or her culture, environment, and stage of personal development. Today, as the increased use of IT has created new challenges, ethical conduct, situational ethics, and morality are still debated. Below are three models that when considered together, provide a good overview of ethical concepts.

1. The Golden Rule

Whether elicited from Confucius, Aristotle, or a dozen other major religious and philosophical personalities, the principle of treating others the way you want to be treated often reveals the best choice to the decision maker. [Ref. 3, 4] This "golden rule" establishes a baseline for behavior in that it calls for a person to be concerned with the well being of others as well as acting for his or her own benefit. The use of this rule requires that the decision maker place himself or herself in the shoes of the person affected by the decision, resulting in introspection during the decision making process. As examples, if you do not want to be lied to or deceived, do not lie to or deceive others. If you want others to keep their commitments to you, keep your commitments to them. However, this standard alone does not work well for complex situations in which more than one choice may be perfectly acceptable. Take for instance the outcome of a business

decision that will affect two people. Neither of these people have knowledge of the dilemma faced by the decision maker. Action One will adversely affect the decision maker's business colleague but provide benefit to a long-time customer. Action Two benefits his business colleague but adversely affects his long-time customer. Either action, taken separately, would be considered ethical and acceptable in general. The consequences of the decision maker's action cannot provide equal benefit to the affected parties; therefore, the framework provided by the golden rule is too simple to apply to this situation. [Ref. 5]

2. Utilitarianism

Two British philosophers, Jeremy Bentham and John Stuart Mill, developed utilitarianism as an ethical model in the early 1800's. Utilitarianism is a consequence-based theory, stating that the only real factor a person should consider when making a decision is the consequence of the action and the number of people positively affected. The right (or good) choice is the one that provides the best outcome for the majority of people. At the basic level, this theory has the decision maker focusing on the consequences of his decision, looking for the best solution for all affected parties.

Human nature makes it difficult to determine what choice provides the most positive benefit. There is no universal scale with which to measure the utility of a decision with regard to its overall effects. It is easy for consequence-based decisions to become situational, with the decision maker rationalizing actions for a self-serving purpose. For example, a major auto manufacturer may have two options: The company can install improved backseat seatbelts at a cost of \$120 million; or it can continue to install the current seatbelt, get a little bad publicity for the decision, and save \$120 million. The statistics indicate that the change in seat belt installation would save less than 20 lives per year compared to current equipment. In this example, how are the lives of 20 people measured? How does the company arrive at the decision to maintain status quo? Focusing on the consequences of a decision first does not necessarily create situations that are conducive to choosing the most ethical path when the less ethical path can be reasoned to be the better choice in general. [Ref. 6]

3. Pluralism

As a theory based in doing one's duty, pluralism holds that decisions should be made out of a sense of duty to do the right thing. According to this ethical theory, as rational beings, humans are able to resist impulse and do the right thing absolutely, regardless of the consequences. The concept of duty within this theory is that of doing the right thing with the right attitude for the right reason. Proponents of this theory espouse that the duty to do the "right" thing is absolute, without exception, regardless of circumstance. This is where the opponents of this theory take issue. Nothing can be considered absolute in the arena of personal human interaction because of the innumerable variables involved. For instance, if the absolute rule is to tell the truth, one could not lie or deceive a kidnapper when asked to tell the whereabouts of the person for whom he or she is looking. In this instance, telling a lie provides a better outcome to a situation and should not pose an ethical problem. Rational people exercising good judgment should be able to tell when exceptions can be made. [Ref. 6]

The models above illustrate the very basics of ethics and ethical theory. Other models include: Contractarianism, which espouses an implied contract between society and government concerning civil and personal rights and responsibilities; [Ref. 6] and the Josephson Institute Ethical Decision Making Model, which uses the Golden Rule as a baseline, then combines associated aspects of utilitarianism and pluralism into a model that attempts to eliminate the shortcomings of all three. [Ref. 5]

Ethical models aside, individual attitudes and convictions of right and wrong, good and bad are the product of upbringing, personal development, education, and other factors. All of these influence the decision maker's perspective and his or her ability to make ethical decisions effectively.

B. ETHICS AND TECHNOLOGY

Now that some ethical models have been discussed, what are the issues that tie ethics and technology together and how has the emergence of technology created new ethical dilemmas? In his paper “What Is Computer Ethics,” James Moor wrote:

Computer ethics is not a fixed set of rules which one shellacs and hangs on the wall. [but] it requires us to think anew about the nature of computer technology and our values. [Ref. 7]

Establishing rules and regulations is only one step in the oversight of the virtual world rising up around us. Moor writes that establishing rules does not fix the issue of poor computer ethics. Delving into the nature of technology and personal values creates a perspective not imagined by theorists prior to the information age.

Individual values and beliefs are ingrained, starting from childhood, shaping the way we view the world, how we establish right from wrong, and creating the convictions that motivate our actions. Values such as trust, responsibility, respect, judgment, and honesty are foundations that we rely on in building our convictions and the guidelines we use to govern our actions. When applied to the computer environment, the authors believe decisions should be made in the same way.

Consider the following news articles and statistics from Websense, Inc, a worldwide leader in employee Internet management solutions:

Websense Inc. reports that the number of pirated software and hacking Web sites has spiked more than 240 percent in the last year alone, now totaling 5,400 sites representing 800,000 Web pages. According to Wordtracker, pirated software terms have risen to the top 15 in recent months, joining "sex" and "MP3" as some of the most commonly typed phrases in search engines. [Ref. 8]

Nearly two-thirds of companies nationwide report disciplining workers for misusing the Internet while working. And a third of those companies surveyed—ranging in size from 6 to over 150,000 employees—have terminated workers that use the Internet to loaf. [Ref. 9]

Secret monitoring by the U.S. Treasury Department of Internet use among Internal Revenue Service employees found that activities such as personal e-mail, online chats, shopping and checking personal finances and stocks accounted for 51 percent of employees' time spent online. The top non-work Web activity favored by IRS employees was going to financial sites.

Chat and e-mail ran a close second, followed by miscellaneous activities (which included visiting adult sites), search requests, and looking at or downloading streaming media (reported in the Chicago Tribune). [Ref. 10]

The examples above appear to indicate that, for many, the application of the values discussed previously do not translate into the IT world. Consider the following verbs and their connotations: cheating, stealing, trespassing, spying, and misappropriation. These words conjure very negative connotations when discussed in general conversation. In Table 1 below, note the parallel IT terminology. The language difference is apparent when viewed comparatively. Actions in the IT realm parallel the actions in the real world, though they are referred to differently. As the above articles indicate, a sizeable number of people do not feel as restrained by the new verbiage.

General Terminology	IT Terminology
Cheating	Copying, plagiarizing
Stealing	Copying, burning (as in copyrighted CD's)
Trespassing	Enumeration
Spying	Monitoring, sniffing, surveillance
Misappropriation	Misuse, unauthorized use

Table 1. Terminology Comparison

To illustrate, consider the practice of cheating on one's income taxes. Although tax evasion has been a long-time problem for the IRS, there is no great proliferation of literature or web content on how to best cheat Uncle Sam out of his share of our earnings. Comparatively, the practice of pirating copyrighted software is widespread, even though it clearly cheats software developers. In this comparison, why is there a disconnect between the real world and the world of IT? One possible reason is the perception of the consequences involved in each case. On one hand, the penalty for tax evasion is severe, and the Criminal Investigation branch of the IRS actively pursues those suspected of cheating with a force of nearly 2800 investigators. [Ref. 11] On the other hand, software developers have no effective way to enforce copyright infringement. The chances of

being punished for copying software are small, particularly if a person is making single copies for personal use. This is just one example that illustrates how the choices people make concerning technology vary greatly from the choices they make in the real world, even though the actions taken are similar, if not exactly the same.

Does technology present new ethical dilemmas not previously encountered? Some researchers believe that technology does not create new ethical problems but merely puts a new “twist” on old ethical questions. Others believe that technology creates completely new dilemmas due to its very nature, similar to the issues the medical community has had to deal with in areas of sustaining life support systems, organ transplantation and donation, artificial insemination, and in vitro fertilization. [Ref. 12]

Yet another explanation could be that many people are ignorant of the design, capabilities, and the usage of IT, and its potential to do harm. As stated in the introduction, 46 percent of Americans do not have access to the Internet. One could assume that percentage is declining as the price of technology decreases and the importance of technology in everyday life increases. With this observation, one could argue that the growing numbers of new Internet users are on the low end of the learning curve when it comes to IT and its proper use.

C. MILITARY APPLICATION

Having discussed ethical models and having identified the technological context for many modern ethical dilemmas, we now turn the discussion to the applicability of these issues to our military environment. As the military has done many times before when dealing with issues that appear to be straightforward, it applies its ideological prudence by creating policy and regulation to resolve issues. Sometimes these decisions have unexpected consequences. For example, in the fall of 1998 the Deputy Secretary of Defense issued a memo directing all units within DoD to significantly modify the content displayed on the World Wide Web in an effort to reduce the vulnerabilities associated with displaying information on the Internet. [Ref. 13] Not only did the intended information come down, but also E-mail addresses, phone numbers, and other pertinent information that people needed to conduct daily business. Hundreds of websites were

shut down because the policy did not clearly state who, what, and how things needed to be accomplished. This policy caused unnecessary work for many people in DoD.

Although every effort is taken to prevent it, the fact remains that computers and information technology create ethical issues that result in policy vacuums that cannot be addressed with policy in a timely manner. The specific regulations and policies that are issued starting at the highest command and then subsequently followed by each subordinate command identify the “official” and “authorized” use of IT assets. These regulations and policies are a good first step toward providing guidelines for handling issues related to IT use, but they fall short of addressing the decision making process required when the regulations cannot specifically address all possible situations personnel are faced with—especially those that require ethical discretion. These ethical issues cannot be resolved without a full understanding of the kinds of ethical dilemmas that IT creates.

The idea of doing one’s duty and serving one’s country, combined with the notions of honor, courage, and commitment create the foundation upon which all service members must make decisions. No matter how well a service member is attuned to the “military way of life,” there will always be the desire to put one’s own well-being first. Basic Training and Officer Candidate School are designed to teach individuals to deny that instinct and sacrifice personal desires for the good of the unit. However, the specific application of self-sacrifice is not directed toward actions taken in cyberspace.

Military organizations are characterized by a distinctive culture; for example, the unique uniforms, specialized language and jargon, and distinct customs and traditions set the military apart from society in general. This culture, by design, permeates areas of personal as well as professional life. There has always been a subjugation of rights by those in the military. Expectations of privacy and personal rights differ from those outside the military. The right to privacy provides examples that can be directly related to the IT world. Deployed sailors and Marines live in open barracks and share close quarters on ship. In these instances, there is no expectation of privacy. No civilian would readily volunteer for such a reduction in privacy. The right to privacy in the military has expanded some with the advent of apartment-style barracks, but personnel

are still subject to unannounced inspections and regulations that govern on-base residency. This privacy issue correlates directly to the IT privacy issue. All DoD computer systems are subject to monitoring, regardless of who is using the system. [Ref. 14] This type of universal monitoring is not commonplace outside of military organizations, but is common within the military.

The complicated makeup of military organizations results in ethical challenges; active duty military, civil service, and contract personnel have different perspectives of the organization and each apply the value system they hold accordingly. For instance, the civil servant's viewpoint may not be one of duty to country but to execution of a job description. Training programs, education and awareness, strict enforcement of existing policy, and leadership are all pieces of the solution to the unethical behavior we see occurring almost daily. Leadership's role is one of mentor and teacher, by instruction and by example. Leadership must direct each of the above ethical perspectives toward a single focal point, so that the best ethical decision for the organization and the individual is one and the same.

No ethical discussion in a military context would be complete without discussing core values. Our core values of Honor, Courage, and Commitment apply to all aspects of life. Whether in uniform or out, on or off duty, in formation or in cyberspace, the general characteristics that are espoused during entry-level training into the military should carry over in the IT world. Our core values are taught early in military careers. Just as our individual values solidify over time, so too must our core values, shaping the way we see ourselves as service members, influencing how we perceive our responsibilities and duty, and creating the ability to make the right decisions for the right reasons. Core values are an integrated part of individual values and should be applied to the IT world.

At present, senior military leadership has relied heavily on basic training (Boot Camp) to change the attitude of the individual to fit the needs of the service. This has been successful for the majority of military skills, but the world of computers has been left out. Indoctrination into the military teaches young recruits how to eat, sleep, dress, walk, and talk, but it does not address the use of DoD computers, networks, and printers. This omission may not seem critical, but at some point individuals must be instructed in

the use of government computing assets. People are a reflection of their culture, and unless all military personnel are versed in what is expected when it comes to the appropriate use of government computers, problems will continue and possibly grow.

When dealing with IT and the Internet environment, traditional ethical concepts apply; only now, they require a bit of translation. In general, users have not viewed the world of computers as “the real world.” Hackers, “script kiddies,” and computer professionals have developed technical expertise which enables them to commit cyber crimes or do serious damage to systems. It has been commonplace in current news to hear about people caught in cyber crimes, who, when questioned about the crime, typically respond that they did not think they were doing anything wrong. This view of the IT world is held by many of the young men and women now joining our armed forces. Changing these views through training and awareness is key to building a force that is not only competent in IT usage but is aware of how ethical conduct is applicable to the realm of IT. As technology continues to develop, becoming more and more complex, everyone needs to make better decisions when faced with ethical dilemmas.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE CONTEXT OF INFORMATION ETHICS

Information ethics is a relatively new field of study and is growing in relevance. The first part of this chapter provides a look at the issues surrounding the increasing importance of information ethics. Many of the circumstances regarding IT and its use faced by the corporate world and American society in general are slightly different than those encountered in the military and in particular DoN. In the second part of the chapter, we:

1. Examine the activities that the Navy and Marine Corps have concern with regard to IT ethics, primarily instances of unauthorized use,
2. Explain the categorization of users in the development of our training materials, and
3. Outline the IT ethics concerns that the authors believe leadership should be aware of.

We focus on these three areas to provide the building blocks of the training materials developed as part of this thesis.

A. A SOCIETY OF TECHNOLOGY

As a new area of applied ethics, information ethics is fast becoming a topic that corporate America, society, and the DoN cannot overlook. The development of new information technologies during the past two decades has resulted in challenges concerning the regulation of technology, the management of information, the appropriate use of technology, and the effects of technology upon society. The ubiquitous nature of electronic communications and the Internet makes the topic of information ethics one of interest for any organization that relies upon these technologies to conduct day-to-day operations.

Even in its infancy, information ethics has been an area of study in which many differing interpretations are possible. As previously noted, there are those who believe that technology creates completely new ethical situations, while others believe that computing technology simply transforms traditional ethical dilemmas. The authors believe both to be the case. Regardless of the perspective, the study of information ethics permits one to identify and analyze “the impacts of information technology on social and

human values.” [Ref. 12] The Information Age has brought about situations and choices of action that are new to human experience. Ethical behavior in this new context requires that we understand how these new situations test the way we exercise our ethical judgment and forces us to address new questions.

Because technology and the Internet are revolutionary, widely available, and rapidly evolving, numerous issues need to be addressed. Several concerns are central to the problem of information ethics: the right to privacy; copyright protection; the collection, stewardship, and use of information; and cyber crime. We will address these key issues here, both from the general and from the military perspective. In addition, we describe what the military has done to address the concerns or what the military could do to address them.

1. Right to Privacy, Workplace Surveillance, and Appropriate Use

Prior to discussing privacy, we must first look at its development. The modern notion of an individual’s right to privacy in the United States did not come about until 1965 in the U.S. Supreme Court decision of *Griswold v. Connecticut*. In a ruling that overturned a Connecticut law making contraceptive use illegal, the U. S. Supreme Court opinion stated that various guarantees contained in the Bill of Rights, specifically the First, Third, Fourth, and Fifth Amendments, create “zones of privacy” for every citizen. [Ref. 15] The Supreme Court has broadly defined privacy as the right of the individual to control the dissemination of information about oneself. In Common Law, protection against the tort of “intrusion” is also applicable. This tort states that the right to privacy is invaded by the unreasonable intrusion upon the seclusion of another. [Ref. 16] In summary, while the Supreme Court ruling provides a basis for privacy arguments, the extent of the right to privacy and the Constitutional basis for privacy still provides a topic for argument by both conservatives and liberals.

The applicability of the common notion of a right to privacy in the military is not so straightforward. An individual’s right to privacy differs once he or she enters military service. The interests of the service outweigh the interests of the individual. This is not to say that sailors and Marines have no right to privacy, just that their rights are

subjugated by what the military determines to be necessary to the execution of the task at hand. With mission accomplishment as the primary focus, our military culture has developed a restricted view of individual privacy, ranging from being subject to surprise personnel inspections to being monitored on workplace computers.

The right to privacy has been a high visibility topic in the last few years. Recent surveys have found that 79 percent of Americans were either very concerned or somewhat concerned that a fellow American might violate their personal privacy. The same percentage of those surveyed thought there would be less personal privacy 25 years from now than we currently enjoy. [Ref. 17] Dilemmas in organizational policy have emerged related to policies for E-mail monitoring and the protection of personal data. E-mail monitoring and the surveillance of Internet use in the workplace have received extensive publicity in recent years.

The concerns surrounding corporate E-mail accounts have led to highly publicized firings and lawsuits, forcing employers to create policies concerning E-mail use in the workplace. In 1991 Nissan Motor Corporation fired two employees after they had been caught sending sexually explicit E-mails. The court battle that ensued resulted in a favorable ruling for Nissan, partly because the company had an E-mail policy in place and had explicitly stated that employees' E-mails would be monitored. [Ref. 18]

In the case of *Smyth v. Pillsbury*, an employee was fired for communicating derogatory comments over the company's E-mail system. Judge Charles Weiner presiding over the U. S. District Court for the Eastern District of Pennsylvania rejected the claim of the employee that the company had violated privacy laws. The ruling revealed that no reasonable person would consider the action an invasion of privacy. The Court decided that the company's interests in managing its network outweighed any privacy interest. [Ref. 18]

The DoN likewise has used government E-mail to prosecute cases. According to Major Greg Gillette, the Military Justice Officer at the Judge Advocate Office in Quantico Virginia, the policy within the Joint Ethics Regulation (DoD Directive 5500.7-R) to monitor all computer use makes any E-mail correspondence admissible at a court martial. Cases have been prosecuted involving E-mail containing pornography and other

unauthorized material such as hate groups' material. Cases may also use E-mail as corroboration of other crimes committed, much like evidence gained using a wiretap; the difference being that the regulation allows the admissibility of E-mails without any special permission to gain access to those E-mails. [Ref. 19] These three examples directly illustrate the need for ethics in the context of IT, be it a question of fairness in monitoring or one of appropriate use of E-mail.

The issue of E-mail privacy can be viewed in the following way: Before computers were networked, employees had to communicate in person or via telephone with co-workers and clients. Employees had control over who was listening to what they were saying. Similarly, mail correspondence has always been private; the addressee being the only person authorized to open and read the contents. Because person-to-person communication of this nature has historically been a personal and private activity, people naturally assumed that E-mail correspondence was private also. From the employers' viewpoint, however, E-mail use is an issue of company time and resource use. Therein lies the dilemma. Whose viewpoint is more correct, that of the employee, or that of the company? This cannot be answered simply by asking what "right" is, because there has not been a defining notion of what "right" should be. The military context leads to a more clear-cut answer. When a sailor asks this question, the answer is apparent: the government's viewpoint and resulting policy is the "right" way to approach E-mail use on government networks.

Right-to-privacy issues extend beyond the interception of E-mail sent on company computer accounts. Workplace surveillance is easy to conduct with current technology. Telephone monitoring has been routine for many years to ensure quality of service, but new technology has created much more efficient ways of observing employees' on the job activities. Sniffers, software that monitors network data traffic, can read everything that comes into the network and can trace the traffic to a specific workstation. Network monitoring software has become sophisticated enough to monitor the keystroke activity of every computer on a network. The practice of logging keystrokes as a measure of productivity would appear to be extreme, but when statistics like the ones involving the IRS investigation from the previous chapter are reported, employers see this as a way to prevent misuse of network assets. [Ref. 20]

A seemingly more legitimate use for keystroke logger software is law enforcement's use of this technology in the investigation of criminal activity. However, even this practice has its challenges. Current wiretap laws are having a difficult time keeping pace with technology. Court challenges result in judges making the decisions concerning the acceptability and validity of using this type of technology. In 2001 Donald Haneke, a U. S. District Court judge in New Jersey, ruled that the FBI did not require a wiretap order to use a keystroke logger in an investigation involving illegal gambling. [Ref. 21] This example requiring judicial review demonstrates that the issues involved in the ethics of privacy are complex and not easily answered.

In any organization, the appropriate use of a corporate resource is a concern for management. While the use of surveillance technology is a growing concern for workers, the low cost of such observation makes network monitoring a viable option for companies concerned with how their employees are spending their time and using company assets. The cost of monitoring employees with readily available commercial software is estimated to be \$5.25 per employee per year. [Ref. 22] Companies spend enormous amounts of capital building reliable networks to conduct business. To protect their investment, appropriate management policies must be put in place. Even so, organizations cannot create policy that covers all possible aspects of computer use.

Studies show a majority of employers lack a comprehensive plan of action for policy development. While 74 percent of employers report using some form of electronic monitoring, only 52 percent have written policies regarding E-mail use. The same percentage of employers offers no training for personnel in the appropriate use of E-mail and no guidance regarding what inappropriate use might be. [Ref. 23] The training of employees on what is considered appropriate use is the first step in achieving a balance between monitored use and personal privacy. The Defense Department's concerns are so strong that a blanket policy of monitoring at all times is used to protect network assets from unauthorized use. The training CD developed as a result of this study is meant to augment that policy by demonstrating its relevance in day-to-day activity.

At the individual level, the question of appropriate use of information technology must be answered with the application of individual ethics. If employees applied IT

ethics training to their actions on company networks, less misuse of company computing power would occur with a consequential reduction in the need for monitoring. Teaching employees what constitutes appropriate and inappropriate actions while using the network would be a step in providing both employer and employee with the comfort level they seek in the workplace. In the next chapter, individual decision making will be emphasized as a necessity in dealing with the complex ethical issues created by technology.

The viewpoints of the employee and employer are only two of three possible perspectives. The government vantage point is also a factor concerning the protection of personal privacy and employers' ability to monitor their employees in the civilian sector. In May of 2001 Federal Appeals Court Judge Alex Kozinski ordered the shutdown of software used by the Ninth Circuit Court of Appeals that tracked the online activities of all employees. The policy that Judge Kozinski rescinded was one that stated "employees had no expectation of privacy at any time while online at work." [Ref. 24] He and the general public believe that this type of policy is unreasonable. The judge in this case thought this policy to be unfair, perhaps even unethical. This case triggered Congressional interest in unrestricted workplace monitoring; specifically, concern that such policies might create low employee morale, an atmosphere of distrust in the workplace, and violate employees' reasonable expectation of privacy. [Ref. 24] These three perspectives and the concerns that accompany them demonstrate that the practice of workplace surveillance and electronic monitoring of employee activity present an ethical predicament that is difficult to solve.

Reference has been made to the military perspective and current policy, and how they differ from those of industry. The paragraph below contains specific verbiage regarding network surveillance.

DoD employees shall use Federal Government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. [Ref. 14. Sect. 2-301.a.3]

Given that the policy points out that simply using a government computer gives consent to monitor, it is reasonable to assume that there is no expectation of privacy when

using government computers. To supplement this regulation, each command within DoD is required to create a disclaimer statement that will be seen prior to attempting to log into a computer. Below is a copy of the disclaimer currently used at the Naval Postgraduate School:

This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

Although this statement deals with security and survivability issues, it is explicit in the right of the government to monitor any activity by anyone on the network. While privacy issues and surveillance questions continue in corporate America, workplace monitoring in the Navy and Marine Corps is well defined, developed by the government for quality system management, to provide adequate security, and to ensure authorized use.

2. Respect for Intellectual Property

Encyclopedia Britannica defines copyright as “the exclusive, legally secured right to publish, reproduce, and sell the matter and form of a literary, musical, dramatic, or artistic work.” [Ref. 25] The first codified application of copyright in the U.S. was in 1790. Since then, the Copyright Act of 1790 has undergone over a dozen significant changes and has been affected by twenty years of case law; changes such as the protection of audio recordings, software, and digital audio manufacturing have been made. [Ref. 26] Copyright laws first appeared as a result of growing use of a 15th century

technology in Europe – the printing press. In 1710 the British Parliament's enacting of the Statute of Anne created copyright protection for literary works. It is appropriate that the origins of copyright followed early technological advancement, because the challenges that copyright laws face today are largely due to current advancing technology.

Although the topic of copyright infringement is not limited to a discussion of technology, the new and more efficient ways of creating, reproducing, manufacturing, and disseminating intellectual property has allowed an old problem to grow to unmanageable proportions. Some software industry experts estimate that over half of the software in use in the United States is unauthorized. Overseas, the estimate grows to 90 percent. [Ref. 27] The power of the Internet has enabled global growth of copyright infringement. This problem is not limited to the copying of software, but also the plagiarizing of others' works found on the Internet as well as the use of databases and the data they contain. The Internet has made it much simpler to find information, easier for individuals to copy it, and to use it without attribution.

The meager enforcement of copyright laws is a large reason for the abundance of illegal software copying. It is simply too difficult and expensive for software companies to track down, prosecute, and recover losses from those individuals making illegal copies of software. The punishment for plagiarism is largely limited to the academic community. The punishment imposed by academia around the U.S. varies from institution to institution. For students, punishment can range from receiving no grade for the work and receiving a letter grade lower for the course involved to suspension or expulsion from the institution. [Ref. 28] In cases of faculty misconduct, suspension or dismissal may occur, but it is dependent upon the severity of the violation. [Ref. 29] Outside academia, copyright infringement of this sort carries no real threat of punishment by the legal system. The laws will never be able to fully protect intellectual property; we depend upon the ethical behavior of the vast majority of individuals to ensure that intellectual property is protected.

Generally speaking, the author or creator of some form of intellectual property is the owner of that property. Copyright law protects that property from being used without

permission. [Ref. 30] The ethical dilemma created for the purpose of our discussion is whether or not to abide by copyright law; either by paying for use as required (in the case of software) or by attributing ownership to the creator (in the case of literary work.) The decision to avoid paying for software or not attributing a quote to another author is not a difficult one for some and is a complex one for others. At the heart of the matter is the question, “Should the creator, whether individual or corporate, be treated fairly for use of his or her creation?”

Look at the issue of software copyright from a utilitarian perspective. From this vantage point, it would appear that allowing an unrestricted number of copies would be beneficial (cheaper and more widely available) to the greatest number of people, therefore making it the best option available. The programmers who developed the code would disagree with the utilitarian approach, but the benefit that the majority received from the unlimited copies would outweigh the concerns of the creators. Conversely, if the golden rule is applied, the perspective changes greatly and now it appears that copyright is a valid way to protect an invention. Once a person considers something from a personal standpoint, the stakes become more important. Application of ethics in the technological world is complex and requires someone not only to understand all the pertinent information before hand, but also to weigh the effects of a decision prior to making it.

The issue of software copyright enforcement within DoN is addressed by limiting access to hard copies of software, limiting access to setup files on the desktop, and the use of enterprise wide licensing when allowed. The illegal copying of software for any reason is nothing more than stealing. It can be addressed through the training of service members in the area of copyright laws, personal and organizational liability, and the tarnishing of the service’s image if illegal activity of this type takes place.

3. Collection, Stewardship, and Use of Information

In this era of computer networks and the Internet, information is nearly flowing at the speed of light. While concerns about privacy abound, there are other issues. Questions about organizations collecting information on customers and clients include:

1. What information is being collected?
2. How is the information being collected?
3. Why is the information being collected?
4. How is the information being stored?

Financial information, healthcare data, public records, marketing sales lists, and buying and spending habits are gathered and stored by various organizations. [Ref. 31] All of this information is being collected via purchasing trend records, website “cookies,” and the sale of database contents. The information is collected because it is more manageable in digital form than on paper; it is cheaper to maintain, easily organized, and more flexible for research and marketing use. Concerns about how the information is stored revolve around the security of the information. The government and the public are faced with determining what information may be gathered and how it may be used. At what point is the information collected about an individual no longer his or hers, and does he or she ever lose ownership of it? [Ref. 31] Government concerns regarding this issue are great; a search of Congressional documents in May 2002 found over a dozen Bills initiated since 1999 regarding information privacy and policy to safeguard consumer personal information. [Ref. 32] How collected information is used and abused is a concern to everyone in this IT dominated world.

With the enormous amount of personal information being collected, concerns about the protection of that data abound. [Ref. 31] Information can be a powerful tool; in the wrong hands, it can be very damaging. Consider the growing problem of identity theft. In an IT context, identity theft occurs when a criminal steals (from some type of electronic database) someone’s personal information: a social security number, credit card number, or other personal information. The thief then uses that information as his or her own. [Ref. 33] The number of identity thefts reported by banks and other financial institutions more than doubled in 2000 (from 267 to 600) and continued to rise in the first one-third of 2001. [Ref. 34] The global marketplace for stolen credit card numbers has continued to grow as technology advances. The theft of credit card numbers has been made simple due to the storage of the information in digital form on merchants’ servers. Hackers can break into a server, gain access to thousands of credit card numbers at a time, steal the numbers, and sell them online for a lucrative profit. All of this can be done without ever breaking into a physical space. Current reports estimate that online

credit card fraud costs merchants close to \$1 billion a year. Although efforts are made to protect consumer information, they are inadequate. New attacks with more powerful hacker tools continually threaten data security. [Ref. 35] Consequently, people are worried about the warehousing of personal data and what actions organizations are taking to protect their information.

The stewardship and use of information is not limited to the business world. The growing amount of information collected by states and the Federal Government is also a target that can be exploited. For example, consider a proposal to place voter registration information online. The online information, which would contain the voter's name, address, county, and possibly phone number, as well as personal demographics, would be useful to government personnel who use the information as part of their jobs. It would be useful to the area voters, making it easier to keep their information up to date. The online information would also be useful to the local politicians' campaign personnel to determine how people in a certain region will vote. All of these are legitimate uses for this type of information. Because all of this information is in the public record [Ref. 36], the requirement to safeguard this information is not the same as that of financial information or health records. Anyone could access this information manually through county or state paper records and use the information for unethical purposes, perhaps criminal purposes. After paper records are digitized and placed in an online environment, it becomes much easier for everyone to gain access to the data, even those who would misuse the information. What is the government's responsibility in this case? Certainly, the government should be concerned with the accuracy of the data due to the nature and usage, but is the government legally bound to protect the information from those who would misuse it? How is access possible for some and restricted for others? Who decides what correct access is? Is the government *ethically* responsible for ensuring the information is only used for legitimate purposes? If so, how is this achieved?

The ethical questions surrounding the collection of data include questions about the method of collection, questions about the responsibility organizations have in the storage of information, and questions about the intended use of the data. Without written policy or guidance, these questions concerning corporate conduct will remain topics of debate. While individuals are protected from credit card fraud, there is no protection

against identity theft. An individual's only protection lies in the ethical conduct of those who have access to such information. Corporate and governmental leaders must make difficult decisions concerning the handling of the ever-increasing amount of data being collected. These decisions will have long-lasting effects on how society handles digital information.

The military perspective concerning the collection and storage of information does not include the use of information for profit or sales research. DoN uses service member demographic information for reports to DoD as well as for recruiting purposes. But these uses are considered part of official government business. The Navy and Marine Corps have safeguards in place to protect service members' pay and personnel records. [Ref. 37, 38, 39] The legacy systems maintained by DoN that contain service member information (Bureau of Naval Personnel (BUPERS) and the Marine Corps Total Force System (MCTFS)) require special permission to gain access. In addition, personnel administrators are trained to protect personal information from unauthorized release. In this case, the protection of individual personal privacy is considered to be in the best interest of the service.

4. Cyber Crime

With the exception of copyright infringement, the discussion thus far has been limited to issues that are difficult to address largely due to the absence of any legal definition of what is right and wrong in the management of IT. These issues exist side-by-side with illegal activities that occur worldwide and affect everyone. Some crimes affect the commercial sector, such as website defacement, database cracking, and the theft of proprietary information, while others affect government organizations such as hackers accessing DoD systems and stealing classified documents. Still other crimes, such as virus creation and dissemination, affect entire countries and in some cases the global community. David Smith was recently sentenced to 20 months in jail for his creation and release of the Melissa virus, which is estimated to have caused \$80 million damage globally. [Ref. 40] Strengthened by the Internet, hackers can commit crimes from halfway around the world, leaving them relatively safe from local prosecution. Cyber crime does not involve the application of ethics since the actions themselves are

illegal. These high tech crimes are included in this dialogue to provide contrast to the gray area we have referred to since chapter one.

Criminal use of technology continues to expand as more lawbreakers become knowledgeable in the intricacies of cyberspace. Computer hacking and illegal software reproduction are not the only way technology is abused. Traditional crime becomes easier to commit with the aid of the Internet and other distributed systems. Electronic money laundering, cyber stalking, and illegal pornography distribution are three of the many ways technology has been corrupted by those with malicious intent. Likewise, career criminals are not the only types of people perpetrating cyber crimes: a teenage hacker experimenting with known operating system vulnerabilities to gain unauthorized access; a disgruntled or discharged employee who finds a way to damage the company network; or a system administrator who uses his access to view personnel salary files. These people are not career criminals, but they are just as dangerous in their misuse of technology.

Efforts of world governments are increasingly being applied to the task of passing legislation to stem the rising tide of cyber crime. [Ref 41] While governments have been working steadily to create laws that enable law enforcement agencies to follow the electronic trail left by criminals, many are lagging behind. A December 2000 report published by McConnell International, a global technology consulting firm, states that less than 37 percent of nations surveyed had taken any action to update their criminal codes to deal with cyber crime. While most influential industrialized countries like the United States, India, and Japan had made substantial progress, the governments of Egypt, France, and New Zealand had taken no action. [Ref. 41] In the U.S., the events of 11 September 2001 resulted in a substantial call for legislation in the areas of electronic surveillance, wiretapping of Internet accounts, and greater immigration tracking by the Immigration and Naturalization Service. All of this activity in IT governance is aimed at increasing intelligence gathering capabilities, expanding governmental power, and preventing future attacks.

This section has discussed the practical and complex aspects of ethics in technology and has shown how ethics are an applicable part of technology management.

In doing so, we created the structure for the next stage of the thesis: the development of training for sailors and Marines in the appropriate use of IT.

B. TAXONOMY OF BEHAVIOR

With the goal of creating IT training for sailors and Marines, the authors conducted research on information ethics and assembled our impressions of the topic based on our Navy and Marine Corps backgrounds. This section will specifically address the gray area behavior faced by DoN personnel, outline the characteristics of the personnel we have set out to train, and describe some leadership issues the authors believe should be addressed.

Consider the figure below:

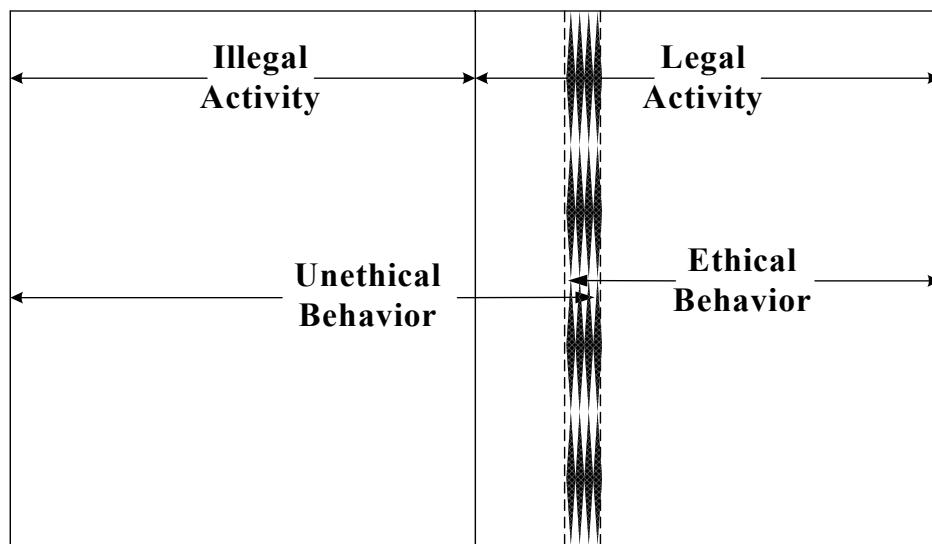


Figure 1. Activity and behavior.

Figure 1 is a diagram that portrays the borders between legal and illegal activity, and ethical and unethical behavior. It depicts the border between legal and illegal activity (the law) as a solid line that, although sometimes debated as to its exact location, is straight and visible. The border between ethical and unethical behavior has no single authority demanding observation of a particular barrier that may not be crossed. It is shown as a wide and blurry line. Within the gray area of the line itself, behaviors may be considered ethical by some and unethical by others, as illustrated by the overlapping

arrows. This is due to the differing ethical norms of each individual. This illustration is applicable to any activity or behavior, not just those involving IT.

In the context of the application of ethics, the IT world should be treated no differently than the physical world. Why is behavior so different in cyberspace when compared to other behavior for some? In 2001 over 60 percent of employees surveyed in a UCLA study admitted to surfing websites for personal use while at work. [Ref. 10] Why do people not understand that, in the eyes of management, wasted time at work equates to loss of revenue for the company? Somehow there is a perceived difference between the realm of IT and non-computer related activities that helps to create ethical dilemmas. We now turn our discussion to those areas where DoN has had problems or where potential problems might lie.

Below is a table of behaviors and actions relating to computer use. In the authors' opinion, all of these fall into the gray area illustrated in Figure 1.

	Typical User	IT Professional	Organizational
Malicious Intent	Password Theft	Identity Theft	Assumed to be non-existent
	Hate E-mail	Mirroring E-mail Accounts	
	Threatening E-mail	Creating 'dummy' accounts	
	Unauthorized access of another account	Hacking (all types)	
	Downloading pornography and other unauthorized web content		
Benign Intent	Downloading MP3s		Monitoring employee E-mail traffic
	Downloading Freeware		Monitoring employee Internet access
	Originating/Forwarding Chain E-mail		
	Use for personal business		
	Conducting personal stock trades		
	Online gambling		
	Sending classified information on unclassified system		
	Personal E-mail subscriptions		
	Paying personal bills online		
	Personal online shopping		
	Forwarding joke E-mails		
	Playing online games		
	Chat room use		

Table 2. Taxonomy of "Gray Area" Behavior

The authors have chosen these activities based on one or more of the following reasons:

1. They match current problem areas within DoN.
2. They are problems encountered by the authors during their 28 combined years of Naval service.
3. They are military-specific problems.
4. They fall into the gray area of activities in which the application of information ethics is well suited.

The behaviors have been categorized in two ways: first, by distinguishing the type of user who would most likely encounter a given situation; and second, by the intent of the action, either benign or malicious. It is understood that IT professionals, such as system administrators or help desk personnel, may encounter all of the activities listed in the first column, but can be differentiated from a typical computer user by virtue of their technical expertise. The far right column lists corporate IT actions currently in place in the DoD that are considered questionable in industry. The table assumes that there is no malicious intent by any action taken by the government (column 3). Most of the behaviors in Table 2 deal with the appropriate use of government networks. The authors believe that this is where the majority of problems lie. Illegal activities are in the minority in Table 2 because illegal activity, such as identity theft and web site defacement, is not a major problem when discussing service member activity.

1. Typical DoN Users

For the purpose of clarity, a rudimentary definition of typical users in DoN needs to be provided. Typical users are considered to be those who do not have administrative privileges, cannot modify any network or node settings, and have no advanced IT training. Typical users range in level of computer competence, from novice to knowledgeable users of software such as word processing or spreadsheet applications. Most typical users have never built a computer, nor would they attempt to take one apart without prior training. They use the computer without the need to understand the inner workings of the box.

The military is a microcosm of society, filled with many young and patriotic citizens, who join the service out of a sense of duty to support the country. The majority

of these people do not set out to disobey orders or be malicious. Their entry-level training provides a general focus for their military lives. Our focus is not to address those who set out to do harm, but those who make mistakes due to lack of training or who wander into the aforementioned gray area and need advice on how to deal with these situations. Many times discussion and contemplation of the situation can provide insights regarding acceptable behavior.

Many of the activities in the typical user column in Table 2 that are classified as benign are perfectly legal and convenient. The use of the Internet for shopping, paying bills, online stock trading, and on-line gambling are perfectly acceptable uses of today's technology from a home computer or a computer located in a cyber-café. Without exposure to government policy, coupled with awareness training, typical users are likely to conduct themselves at work the same way they would at home, with no qualms about their actions.

Consider the viewpoint of the Navy and Marine Corps on these issues. First, every service member is a public servant employed to benefit the country. All activity conducted at work should be official business or least in the best interest of the service and the country. Second, the government has invested a significant amount of capital into creating networks for official government use. Because the Joint Ethics Regulation mandates that government IT equipment be for official and authorized use only, the use of these networks should be limited as much as possible to government business. Lastly, the use of good judgment is paramount in the discernment of what is acceptable behavior on government networks.

2. DoN IT Professionals

As defined in this study, IT professionals include network administrators, helpdesk and Network Operations Center (NOC) personnel, or any personnel who have received advanced IT training or certification, either through official training or personal education. IT professionals can be faced with decisions involving the activities listed under the first column of Table 2, but there are other things they can encounter due to their training and position. The behaviors in the second column of Table 2 fall into the

malicious category because IT personnel should understand how the network should be managed; they appreciate the implications of bandwidth misuse; they are more familiar with the cost of network development and management; and they understand network monitoring. That is to say: IT professionals know better.

With increased knowledge often comes increased responsibility. The knowledge of how systems work coupled with the ability to better utilize network capability implies that IT professionals have the ability to do more harm than a typical computer user. To aid IT professionals, guidelines have been developed concerning the ethical use of computers and the knowledge the IT professional has at his or her disposal. The list below, known as the Ten Commandments of Computer Ethics, contains both broad and specific guidance regarding the use of IT. However, as Moor's quote stated in Chapter Two, just hanging these rules on a wall does not mean that anyone will adhere to them.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not use or copy software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you write.
10. Thou shalt use a computer in ways that show consideration and respect.

Developed by the Computer Ethics Institute, 1992 [Ref. 42]

These commandments were developed to aid and remind IT professionals of the ethical responsibilities that accompany the knowledge their field employs.

3. The Role of Naval Leadership

To provide junior sailors and Marines with the leadership they require, officers and noncommissioned officers must understand the ethical problems their subordinates face. In this context, here are a few matters that leadership should be aware of:

1. The modern workspace isolates individuals with their computer. Contributing factors include individual computers on the desktop, cubicles designed for maximum floor space efficiency, and Internet access at the touch of a button. In small unit oriented organizations like the Navy and Marine Corps, personal isolation is counter to unit cohesion, teamwork, and mission accomplishment.

2. Young sailors and Marines are entering military service with more computer experience than ever before. Their knowledge of computer ethics may not be as developed. Unless properly trained this lack of understanding could lead to misuse of the network.
3. In the Joint Ethics Regulation, there is room for interpretation (gray area) concerning authorized use. Local commanders are allowed some latitude in defining what is authorized. Local commanders should clarify these instances to avoid placing personnel in the position of trying to determine acceptable action.
4. Our research found no single higher headquarters agency oversees IT ethics training in the Department of the Navy. [Ref. 43] One may infer that because of this, IT ethics training is not conducted at any echelon of command. There should be a single point of authority to aid military leadership in the prevention of unethical and unauthorized use of government computers.

The issues discussed above are by no means all encompassing, but they are meant to provide leadership with an exposure to the types of areas about which to be concerned. The very nature of IT development causes issues to change with time. These issues relate to the problems the military is having with IT ethics management. It is important to address them as a first step toward making sailors and Marines better decision makers in the realm of ethical IT behavior.

This chapter identified ethical problem areas in IT to illustrate the importance of IT ethics. The taxonomy of gray area behaviors was developed from the authors' perspective of the problems that exist in the Navy and Marine Corps. This chapter also outlined the target audience for training in IT ethics. Using this taxonomy as an outline of the problems faced by Naval personnel, the authors created Web-based training in the form of a CD-ROM, to be detailed in the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TRAINING AND AWARENESS

Having established a context for information ethics in the previous chapter, we now focus on training and awareness materials. The training section outlines the layout and use of the training CD, provides useful facilitator information, and explains the purpose of having this training as a facilitated discussion group. An overview of the facilitated decision making process is also covered to provide insight into how people arrive at the decisions they make. The awareness section that follows provides information to spark awareness at the local command level that may be expressed in posters, general ethics information, screen savers, and other materials.

A. TRAINING MATERIAL

Training refers to a planned effort by an organization to facilitate the learning and knowledge of specific job-related behaviors on part of its employees. [Ref. 44] The job-related behavior we intend to foster is that of ethical decision making when using government IT resources. The intent is to develop schoolhouse and workplace training and education using a systematic approach to learning that results in improvement of individual and overall organizational effectiveness. [Ref. 45]

Our training objectives are to: (1) improve individual awareness of IT and ethics, (2) to develop individual decision making skills as applied to ethics, and (3) to motivate the individual to apply ethical concepts while using IT resources.

1. iTechs Training CD

The iTechs Ethics Training and Awareness CD was developed to be included in the annual General Military Training (GMT) regimen. The training is all-inclusive, in that the reference material and supporting documentation to complete the training in information technology ethics are provided on the CD.

a. CD Layout

The sections on the CD are: Introduction, Purpose and Objectives, How to Use this CD, What is IT Ethics, the Toolbox, Glossary of Terms, and Contact Information. The illustration in Figure 2 depicts how the training should be presented:

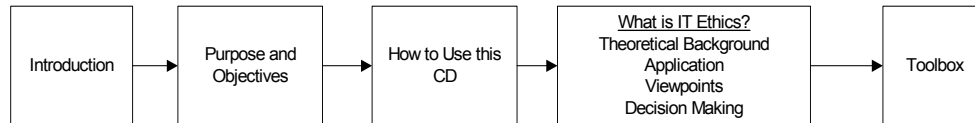


Figure 2. iTechs Training Flow Map

A key element of this training is the Toolbox section on the training CD. In the Toolbox, scenarios illustrate a wide range of ethical situations. These scenarios were designed to initiate facilitated discussion of ethical dilemmas that individuals may encounter while using IT resources.

b. Training Methodology

The training can be offered individually, individually facilitated, or as facilitated group training. Typical IT users (as previously defined) should receive one hour of training. If offered as individual GMT, the facilitator should select seven to nine case scenarios from the Toolbox that the individual student would be required to work through to complete the training. When reading the scenarios, the student should view the dilemmas from each perspective of the characters presented. Doing this helps the student fully appreciate the various aspects of the situations faced by everyone in the scenario. To fit into the annual GMT block, group training for typical IT users should be minimally one hour of training. Because group facilitated training is designed to generate discussion among the students, four to six case scenarios selected by the facilitator are needed to complete group training; otherwise, additional time should be allotted.

It is recommended that IT professionals receive either more than one hour of training or both individual and group training combined over a time period specified

by the local command. For the most comprehensive training, IT professionals undergoing the training should review all the scenarios in the Toolbox.

c. Importance of Lecture/Discussion Format

Although the iTechs training may be conducted in groups or individually, the subject lends itself to group training. The facilitator's role is to present the objectives of the training, the concepts surrounding the ethical use of IT, and to lead the students in discussion of the ethical dilemmas presented in an open forum. To present the material, the facilitator must become familiar with the information provided below and on the CD. He or she should follow the flow map provided in Figure 2 for both individual and group training. Complementing this, facilitator notes are included on the CD to assist the facilitator when presenting the training.

The lecture and discussion method is the most common delivery method for training programs but many training experts still question the usefulness of this training technique. [Ref. 45] The concern is that communication tends to be one-way, resulting in passive learning, in which case students do not have an opportunity to sufficiently grasp the information presented. Another issue is the differing degrees of abilities, attitudes, and interest of the students – and the trainer's ability to instruct a diverse group. To that end, a lecture/discussion method was chosen as the delivery method for iTechs because the results of several studies support the effectiveness of this method as an attitude-changing technique. Complementing the lecture with scenarios provides a dynamic method of training, like that of Socrates and the question to his followers of "What do you think?" enabling the students to develop their skills in analysis and problem solving. [Ref. 45] In this discussion format, the authors believe the groups' diversity enhances individual learning.

2. Decision Making

There is a vast amount of information and literature available in the area of decision making. Therefore, the following definitions are provided for clarity:

Values are guidelines a person uses when confronted with a situation in which a choice must be made. Typically, values that are acquired early in life remain a

basic part of a person's personality; however, values can change over time through experience and education.

Personality is the psychological force or make-up of a person that derives from a person's belief, attitude, needs, and external physical and environmental forces that are called upon to influence a given decision.

Risk can be characterized in terms of gains or losses, in which the decision makers' perceptions of the final outcome is influenced by what they perceive the outcome might be.

Dissonance is internal conflict created by holding beliefs and attitudes that conflict with each other at the same time. Dissonance plays a large role when confronted with a decision that relates to conflicting beliefs. [Ref. 46]

A decision is a conscious choice made among available alternatives. [Ref. 47] Decision making is the process by which an individual identifies problems, opportunities, and outcomes that result from alternatives of a decision that will be made. [Ref. 46] The four factors defined above all play a part in the decision making process and influence the decision maker. Sound decision making is a learned skill; it is developed through years of experience making sound decisions and learning from the mistakes of poor ones. In the context of new ethical dilemmas created by technology, lack of prior experience makes decisions involving behavior in cyberspace harder.

A decision maker will separate his or her decisions into two categories: programmed and non-programmed decisions. Programmed decisions are a consequence of past incidents, whereby a decision maker is able to apply lessons learned to new situations he or she encounters, enabling the decision maker to more easily choose a desired outcome. Non-programmed decisions are different. When faced with new situations, a decision maker does not have the past experience or situational expertise to gain insight into the best alternative. Non-programmed decisions are also sometimes known as intuitive decisions, whereby a decision maker will make hunches, guesses or even estimates to achieve the best outcome for a decision. [Ref. 46] Because this intuitive decision making is done without the benefit of prior experience, the decision maker assumes an increased amount risk in choosing the best alternative.

There are other approaches to decision making, such as a systematic approach. Systematic decision making is an organized, exacting, data-driven process used to derive the best outcome. [Ref. 46] This sort of decision making requires complex analysis of all

known alternatives. Because of the analysis, complexity, and time involved, the authors believe this approach is not the likely choice of decision styles for day-to-day type decisions.

Given existing DoD policy and regulation, coupled with our core values, why are people in the Department of the Navy making unethical decisions when using information technology? There is a certain percentage of people that will assume the risk of going counter to our ethical standard, choosing to blatantly defy existing policy, rule, regulation and our core values no matter what. Others are just not aware that their actions are inappropriate or unauthorized. The majority of sailor and Marines want to do the right thing. For them, we constructed the following steps to aid in arriving at an acceptable outcome when faced with situations requiring the application of IT ethics. If presented with an ethical dilemma a person should ask himself or herself the following four questions. If they are able to answer ‘no’ to all four, their decision will likely fall within the Department of the Navy ethical standards.

Step 1 – Are you aware of any rule, regulation, statute, policy, or directive that would otherwise alter your decision?

Step 2 – Are you aware of any detrimental outcomes or impacts that would result from the decision you make?

Step 3 – Is the result of your decision an outcome that is counter to Department of the Navy core values – Honor, Courage, and Commitment?

Step 4 – Would the presence of your Commanding Officer, Command Senior Enlisted, or direct supervisor change your decision?

B. AWARENESS MATERIAL

Awareness materials are designed to create an atmosphere conducive to the subject being addressed without mentioning the specifics of the subject, using such things as conceptual art and rhetorical questions. Historically, the military has used awareness material to enlighten service members on subjects such as Equal Opportunity, Sexual Harassment, and Drug and Alcohol Awareness. All of these topics are the subject of direct training but are enhanced by the existence of awareness materials. The iTechs awareness materials focus on the concepts discussed within this thesis and on the training CD: (1) the importance of the relationship between IT and ethics, (2) government

surveillance of IT use, (3) better individual decision making and how certain factors influence decisions, and (4) guidance on the ethical use of IT. Graphics that can be used as command bulletin board posters, PC desktop wallpaper, and screen savers are included in the Toolbox section of the CD for local commanders to use as they deem necessary.

Appendix B provides a preview of a few of the materials on the CD.

V. CONCLUSION

The rapid growth of information technology continues to change the landscape of the world we live in. This networked environment has changed the way we work and play, communicate with friends and co-workers, and how the Navy and Marine Corps accomplish their respective missions. The DoN has come to depend upon IT in a multitude of ways, whether it be E-mail servers, workplace Internet access, decision support systems, or satellite links. The ubiquitous nature of information technology has created change in almost every aspect of life in the military service.

As with all major change, questions arise about how such change affects and influences other areas. One such affected element of life is the application of personal ethics and individual decision making in the use of IT. Information ethics has grown as a new area of study concerned with why the application of ethics is different when acting in cyberspace. Technology creates new ethical problems never encountered before and gives new dimensions to old dilemmas. This is the primary challenge for people when applying their ethical norms to IT. These new dilemmas lack policy, regulation, or law to specifically address new circumstances. These new circumstances become gray areas that challenge known ethical standards. Throughout this thesis, arguments have been made to support this notion.

The Navy and Marine Corps, like commercial industry, continue to have incidents of unethical behavior by personnel using organizational IT resources. They vary from unauthorized use of E-mail to malicious behavior by IT managers. These incidents, coupled with the notion that ethical standards somehow change when acting in cyberspace, demonstrate a need to bridge the gap between IT and ethics. The DoN cannot address this issue by creating more policy and regulation. Deborah Johnson agreed: "Law is neither the beginning place nor the ending place when it comes to filling the policy vacuums and addressing ethical issues." [Ref. 2] Ethics can neither be taught from a book nor mandated by regulation; therefore, the solution is to improve individual decision making when faced with ethical dilemmas in cyberspace. This can be accomplished through relevant training and heightened IT ethics awareness.

With the understanding that information technology creates ethical dilemmas and uncertainty about right and wrong, the authors created a plan of action to develop CD-ROM-based training with the objective of teaching personnel how to make better decisions about IT usage. This plan included: identifying the various types of computer users within DoN, creating a taxonomy of gray area behaviors upon which to focus while writing the training scenarios, and creating relevant and effective training built with the intent of exposing the student to the importance of ethics in cyberspace.

The iTechs training and awareness materials are meant for all DoN personnel. Anyone with a computer connected to a network is exposed to situations that may require him or her to exercise sound, ethical judgment that elicit an appropriate response. The iTechs CD provides training for sailors and Marines that is interactive, relevant to their workplace, and flexible enough to incorporate in a variety of teaching situations. The facilitated discussion format lets students interact as a group while addressing issues that are raised through the use of training scenarios. Students will encounter situations involving shipboard and shore command networks, intranet use and Internet downloads, as well as topics dealing with personal and group decision making. Although designed for group training, the variety of topics covered and amount of scenarios provided makes the iTechs CD flexible enough to use for individual training as well. In addition to the scenarios, the authors created a simple four-step decision making tool for IT users to apply when facing ethical challenges. This tool, a set of rhetorical questions, forces the decision maker to confront possible detrimental effects or ramifications of a decision as well as consider what his or her decision would be in the presence of others. The training and awareness tools coupled with group discussion of the scenarios on the CD will prepare service members to address situations they have not dealt with previously. The iTechs training is intended to make these difficult decisions encountered in cyberspace less challenging.

Future study of this topic is germane to the DoN. The iTechs CD is sufficient as a first edition but updates will be required as technology evolves. Revisions might include updates to scenarios to match technological advances, inclusion of interactive video in scenarios and Web-enabled e-learning environment capability. Additionally, research in the effectiveness of this type of “behavioral” training will be required.

As the Department of the Navy becomes more and more dependent upon technology, the individual choices made by personnel can potentially have great impact. Leadership at all levels must take an interest in how personnel behave in cyberspace and understand the effects of their inappropriate actions. Policy guidance issued from higher headquarters concerning government IT use is a first step; the iTechs training and awareness CD bridges the gap between the policy and the situations encountered by sailors and Marines by exposing them to information ethics and its importance. Short of having a programmed decision to rely on, the training provides some insight into new dilemmas encountered, hopefully reducing the number of incidents encountered within DoN.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

This appendix is provided to supply samples of the web pages contained on the iTechs training CD. They are presented in the order they appear on the CD. The final two graphics provide examples of the scenarios encountered in the training.

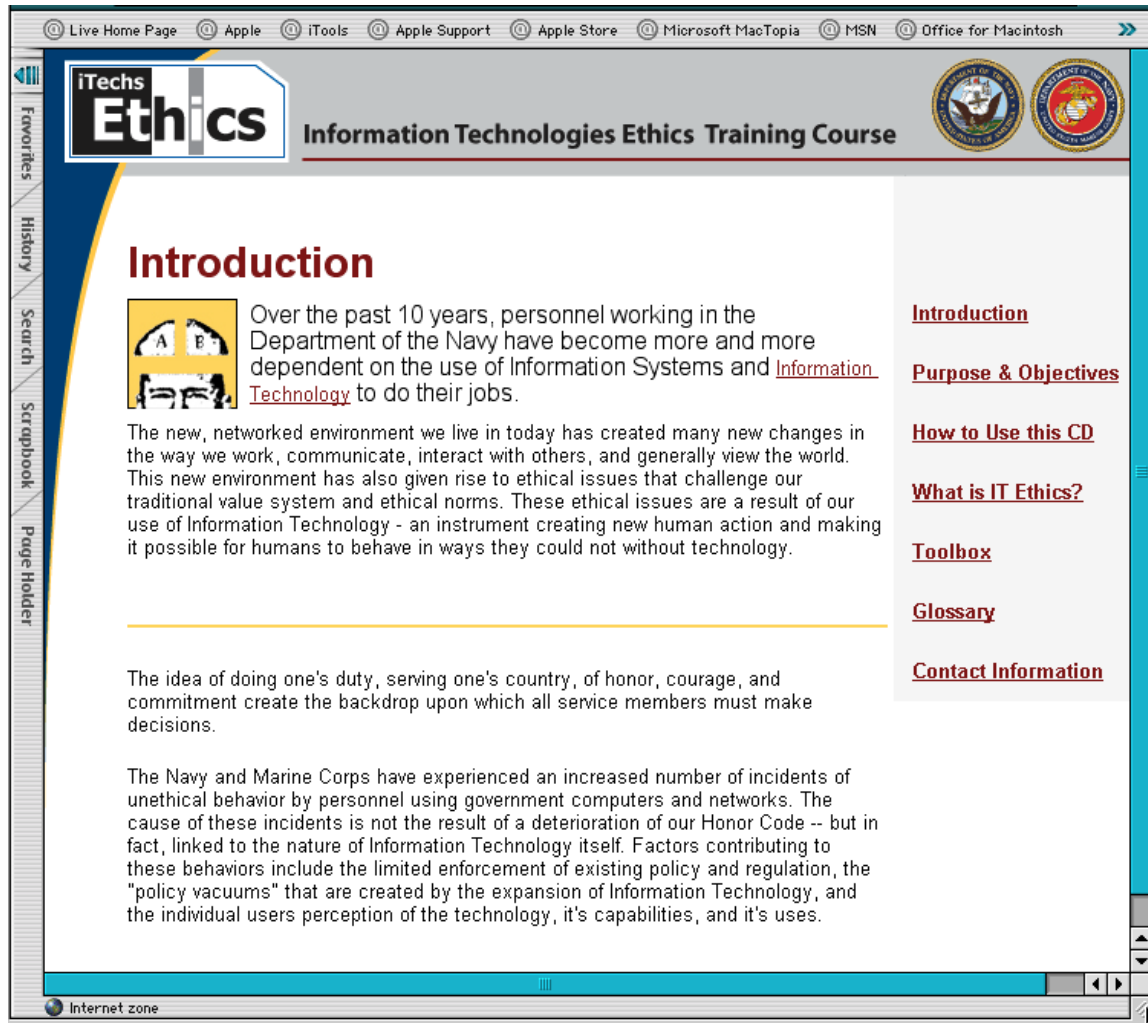


Figure 3. iTechs Introduction Page

The screenshot shows a web browser window with the title bar displaying various icons and the text "Live Home Page", "Apple", "iTools", "Apple Support", "Apple Store", "Microsoft MacTopia", "MSN", and "Office for Macintosh". The browser's address bar shows "Internet zone". The website's header features the "iTechs Ethics" logo on the left, the title "Information Technologies Ethics Training Course" in the center, and two circular seals on the right: the Department of Defense seal and the Department of the Navy seal. A vertical sidebar on the left contains links for "Favorites", "History", "Search", "Scrapbook", "Page Holder", and "Holder". The main content area is titled "Purpose and Objectives" in a large, bold, red font. Below this title, there is a small icon of a person's face with the letters "A" and "B" on either side. The text under the "Purpose" heading states: "The purpose of this training is to provide Department of the Navy personnel with a training tool that furthers their understanding of the ethical responsibilities that are required when using Information Technology and to provide a broad knowledge base that facilitates better decision making when facing ethical dilemmas." A paragraph follows, explaining that the military Honor Code mandates a higher standard of behavior for military personnel than for civilians, and that the training aims to condense available information and combine it with scenario-based dilemmas to provide a concise and informative tool. On the right side of the page, there is a vertical list of links: "Introduction", "Purpose & Objectives" (which is highlighted with a blue background), "How to Use this CD", "What is IT Ethics?", "Toolbox", "Glossary", and "Contact Information". The bottom of the page features a blue navigation bar with a "Home" button and a "Back" button.

iTechs Ethics
Information Technologies Ethics Training Course

Purpose and Objectives

Purpose
The purpose of this training is to provide Department of the Navy personnel with a training tool that furthers their understanding of the ethical responsibilities that are required when using Information Technology and to provide a broad knowledge base that facilitates better decision making when facing ethical dilemmas.

The military Honor Code mandates that military personnel be held to a higher standard of behavior than what is typically expected of our civilian counterparts. In today's military, personnel have more autonomy and are required to exercise personal judgment and decision-making more than ever before. Choices about personal behavior, specifically, making decisions that are ethical and beneficial to the service member and his organization, become more pronounced in cyberspace. The process of effective decision-making is at the heart of this training. Simply pointing to a list of rules in a frame on a wall doesn't provide an individual with the tools to react to situations he or she finds in daily life. There is an enormous amount of information available to Navy and Marine Corps personnel concerning ethics and ethics awareness in the Department of Defense. The goal of this training is to condense available information and combine it with scenario-based dilemmas to provide a concise and informative tool to better prepare the users of this material with the knowledge to deal with the ethical dilemmas that can be faced while using Information Systems and Information Technology.

Objectives

- Identify for the user what Information Technology and [Information Technology Ethics](#) are and how the study of ethics relates to Information Technology.
- Explain how and why Information Technology gives rise to ethical dilemmas that other technologies don't.
- Provide framework for Information Technology users with tools that will assist them in their decision-making when faced with Information Technology ethical dilemmas.
- Make users aware of the ethics policies of DoD and better understand their application.

[Introduction](#)
[Purpose & Objectives](#)
[How to Use this CD](#)
[What is IT Ethics?](#)
[Toolbox](#)
[Glossary](#)
[Contact Information](#)

Internet zone

Figure 4. iTechs Purpose and Objectives Page





Figure 5. iTechs What is IT Ethics Page

Live Home Page
Apple
iTools
Apple Support
Apple Store
Microsoft MacTopia
MSN
Office for Macintosh

iTechs
Ethics


Information Technologies Ethics Training Course

Favorites
History
Search
Scrapbook
Page Holder

What is IT Ethics?

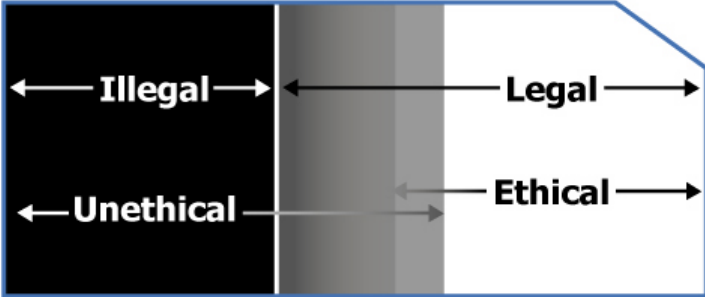
Ethics and Technology



In general, the law delineates what is legal and illegal in everyone's eyes.

On the question of law, there is no gray area, only a single line, to be crossed or to be observed. When the discussion turns to ethical behavior however, the line becomes fuzzy, or wider, with no single authority demanding observation of a particular barrier upon which not to cross.

Consider the illustration below.



The shaded area is the one of concern for our discussion. This illustration is not in anyway limited to the IT world, but clearly the actions taken behind a computer or inside a network are applicable.

Keeping in mind the models just introduced, what are the issues that tie ethics and technology together and how has the emergence of technology created new ethical dilemmas?

Consider the following table.

General Terminology	IT Terminology
Cheating	Copying
Plagiarizing	Copying, Internet search
Stealing	Copying, burning (as in copyrighted CD's)
Trespassing	Enumeration
Spying	Monitoring, sniffing , surveillance
Misappropriation	Misuse, unauthorized use

In general, the actions on the left carry more negative connotation than those on the right. The increased use of IT has been the driving force behind the evolution of terminologies, each change lessening the negative connotation or degree to which the precedent term is received. The change in connotation is not hard to discern when viewed side-by-side. This may help us understand why there is a disconnect between how people perceive the real world and the world on the other side of the computer screen.

Now let's look at IT Ethics from a [Technical Viewpoint](#)

[Introduction](#)

[Purpose & Objectives](#)

[How to Use this CD](#)

[What is IT Ethics?](#)

- [Golden Rule](#)
- [Utilitarianism](#)
- [Pluralism](#)
- [Ethics & Technology](#)
 - [Technical Viewpoint](#)
 - [Organizational Viewpoint](#)
 - [Personal Viewpoint](#)
 - [Decision Making](#)
 - [Behaviors](#)

[Toolbox](#)




[Glossary](#)

[Contact Information](#)

Internet zone


Figure 6. iTechs Ethics and Technology Page

Live Home Page
Apple
iTools
Apple Support
Apple Store
Microsoft MacTopia
MSN
Office for Macintosh


Information Technologies Ethics Training Course



Favorites
History
Search
Scrapbook
Page Holder
5
History
Search
Scrapbook
Page Holder

What is IT Ethics?



Organizational Viewpoint

Military organizations are characterized by a distinctive culture, more than most other organizations.

This culture, by design, permeates areas of personal as well as professional life. There has always been a subjugation of rights by those in the military. One's expectation of privacy, and personal rights are not equal to those outside the military. The right to privacy is an instance that can be directly related to the IT world. Deployed sailors and Marines live in open barracks and share close quarters on ship. In these instances, there is no expectation of privacy. This reduction in privacy is a situation that no civilian would readily volunteer himself to be a part of. The right to privacy has expanded some with the advent of apartment-style barracks, but personnel are still subject to unannounced inspections and regulations that govern on-based residency. This privacy issue correlates directly to the IT privacy issue. All DoD computer systems are subject to monitoring, regardless of who is using the system. This type of universal monitoring isn't commonplace outside the military organization.

Regulations and Enforcement

As it has done many times over when dealing with new issues that appear to be straightforward, the Department of the Navy applies its ideological prudence by creating policy and regulation to address new circumstances. These new policies are typically based on previous paradigms, which may or may not fit the situation. Although every effort is taken to prevent gaps, the fact remains that computers and information technology create ethical issues that result in policy vacuums that cannot be addressed in a timely manner. The specific regulations and policies that are issued starting at the highest command, and then subsequently followed by each subordinate command, identify the "official" and "authorized" use of IT assets. These regulation and policies are a good first step, but fall short of addressing or resolving the problems that occur when personnel are faced with decisions that require ethical prudence.

The letter of the law so to speak is found in DoD Instruction 5500.7-R, which is the Joint Ethics Regulation. Chapter 2 of this Instruction deals with the Standards of Ethical Conduct. Section 2-301 is the appropriate section of the Manual dealing with this subject. You may view the entire document at http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/. This training will reference this instruction as well as others throughout the material.

The regulation, without enforcement, is ineffective. Just as if commanders and the JAG Corps did not enforce the UCMJ, the effectiveness of this regulation is only as good as the enforcement of its contents. Not until leadership plays a part in the enforcement, through example and vigilance, to ensure that the standards are kept, and those failing to abide by them are punished, will the Navy and Marine Corps see a decrease in the amount of misuse of government IT assets.

Now let's look at IT Ethics from a [Personal Viewpoint](#)

Introduction

Purpose & Objectives

How to Use this CD

What is IT Ethics?

- [Golden Rule](#)
- [Utilitarianism](#)
- [Pluralism](#)
- [Ethics & Technology](#)
- [Technical Viewpoint](#)
- [Organizational Viewpoint](#)
- [Personal Viewpoint](#)
- [Decision Making](#)
- [Behaviors](#)

Toolbox

Glossary

Contact Information

Internet zone

Figure 7. iTechs Organizational Viewpoint Page

Live Home Page Apple iTools Apple Support Apple Store Microsoft MacTopia MSN

iTechs Ethics Information Technologies Ethics Training Course

What is IT Ethics?

Decision Making



The process of sound decision-making is a learned skill, taking years to develop.

This section provides the basic elements and definitions of decision-making that will be useful to the users of this training.

A **"decision"** is defined as a conscious choice made among available alternatives. "Decision-Making" is the process by which an individual identifies problems, opportunities and outcomes as a result of the alternatives derived from the decision that will be made. There are several factors that influence an individual decision-maker's ability to make decisions, such as values, personality, the propensity for risk and potential for dissonance.

Values are guidelines a person uses when confronted with a situation in which a choice must be made. These values are acquired early in life and are a basic part of a person's personality.

Personality is the psychological force or make-up of a person that derive from a person's belief, attitude, needs, and external physical and environmental forces that are called upon to influence a give decision.

Risk can be characterized in terms of gains or losses, in which the decision-makers' perception of the final outcome is influenced by what they perceive the outcome might be.

Dissonance is internal conflict created by holding beliefs and attitudes that conflict with each other at the same time.



Internet zone

Figure 8. iTechs Decision Making Page

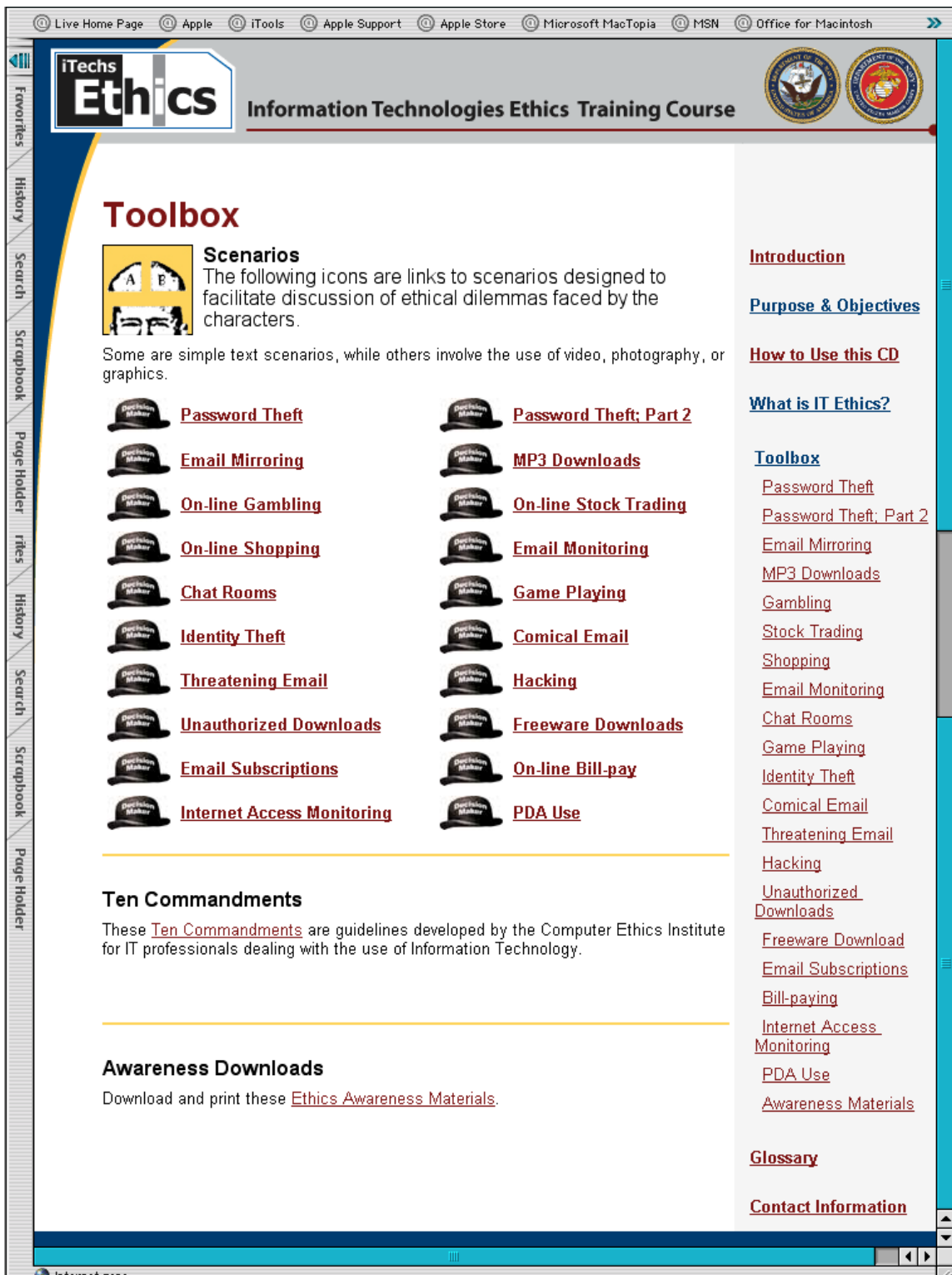


Figure 9. iTechs Toolbox Page

The screenshot shows a web browser window displaying the iTechs Ethics Information Technologies Ethics Training Course. The browser's address bar shows the URL "http://www.apple.com/education/ethics/". The page has a blue and white color scheme. The main content area is titled "MP3 Downloads Inappropriate Use" and includes a "Decision Point" section with two questions. The right sidebar contains a list of topics under the heading "Toolbox".

iTechs Ethics
Information Technologies Ethics Training Course

Toolbox

MP3 Downloads Inappropriate Use

Issues: Network Usage; Security

Chief Davis just bought a new MP3 player to replace his broken CD player. After a few nights at home on the Internet, he realizes that downloading MP3's on his 56k modem takes all night. He knows that the network connection at work is a T1, and is fast enough to download MP3s quickly and easily, especially after working hours.

Decision Point

1. Does Chief Harris download MP3's in the background of his desktop while working?
2. Does Chief Harris return after working hours and downloads MP3's while finishing up paperwork?

Discussion Points/Things to consider:

Chief Harris can get faster downloads at work, but is that an authorized use of the network?

Consider this: What if all owners of MP3 players within the command downloaded MP3's while at work? This would degrade the performance of the entire network due to the amount of bandwidth being utilized by the MP3 traffic. This in turn restricts the amount of data being carried by the network.

What if he comes in after work? No one is using the network then.

Chief Harris can rationalize that MP3's for his player are good for morale.

As with anything downloaded from the Internet, MP3s' can contain viruses, which can be harmful to the network.

Introduction

Purpose & Objectives

How to Use this CD

What is IT Ethics?

Toolbox

- [Password Theft](#)
- [Password Theft: Part 2](#)
- [Email Mirroring](#)
- [MP3 Downloads](#)
- [Gambling](#)
- [Stock Trading](#)
- [Shopping](#)
- [Email Monitoring](#)
- [Chat Rooms](#)
- [Game Playing](#)
- [Identity Theft](#)
- [Comical Email](#)
- [Threatening Email](#)
- [Hacking](#)
- [Unauthorized Downloads](#)

Figure 10. iTechs MP3 Download Scenario Page

The screenshot shows a web browser window displaying the iTechs Ethics Information Technologies Ethics Training Course. The browser's address bar shows various links like Live Home Page, Apple, iTools, Apple Support, Apple Store, Microsoft MacTopia, MSN, and Office for Macintosh. The page has a header with the iTechs Ethics logo and the course title. A sidebar on the left contains links for Favorites, History, Search, Scrapbook, and Page Holder. The main content area is titled 'Toolbox' and features a section on 'On-line Bill-pay Unauthorized Use' with a small image of a 'Decision Maker' hat. Below this is a paragraph about Seaman Recruit Michaels and a 'Decision Point' section with a question. A 'Discussion Points/Things to consider:' section follows. On the right, there is a list of topics including Introduction, Purpose & Objectives, How to Use this CD, What is IT Ethics?, and a Toolbox list with items like Password Theft, Email Mirroring, and Identity Theft.

iTechs Ethics
Information Technologies Ethics Training Course

Toolbox

On-line Bill-pay Unauthorized Use

Issues: Inappropriate Use; Security; Network bandwidth

Seaman Recruit Michaels is a hard charging up and coming Seaman Apprentice that is so squared away he completed all of his personal qualifications through Petty Officer First Class in his first year of active duty. While getting cash out of the ATM, SR Adams notices an advertisement from his bank about paying bills online. Being the squared away sailor that he is, SR Adams thinks that paying bills online is a terrific idea, particularly once underway, but he does not have a PC since he lives in the barracks. Surely using one of the command's computers would be alright.

Decision Point

- Does SR Adams decide to use one of the Command PC's to pay his bills online?

Discussion Points/Things to consider:

What are the ramifications of this decision? What SR Adams is doing appears to be harmless - especially since he has no other means of using a computer to pay his bills.

Introduction

Purpose & Objectives

How to Use this CD

What is IT Ethics?

Toolbox

- [Password Theft](#)
- [Password Theft; Part 2](#)
- [Email Mirroring](#)
- [MP3 Downloads](#)
- [Gambling](#)
- [Stock Trading](#)
- [Shopping](#)
- [Email Monitoring](#)
- [Chat Rooms](#)
- [Game Playing](#)
- [Identity Theft](#)
- [Comical Email](#)

Figure 11. iTechs On-line Bill-pay Scenario Page

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

To use iTechs graphics as a screen savers:

1. Save iTechs graphic files to a local folder.
2. Open Display in Control Panel. (To open Display, click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Display**.)
3. On the **Screen Saver** tab, under screen saver, click **My Pictures Slideshow** in the list.
4. Click **Settings** to specify the folder containing the iTechs images, define picture size, and set other options. **My Pictures Slideshow** scrolls through all the pictures in the folder.

After you specify a screen saver, it will automatically start when your computer is idle for the number of minutes specified in **Wait**.

Click **Preview** to see how the selected screen saver will appear on your monitor. Move your mouse or press a key to end the preview.

The images below are samples of the graphics available on the iTechs training CD.

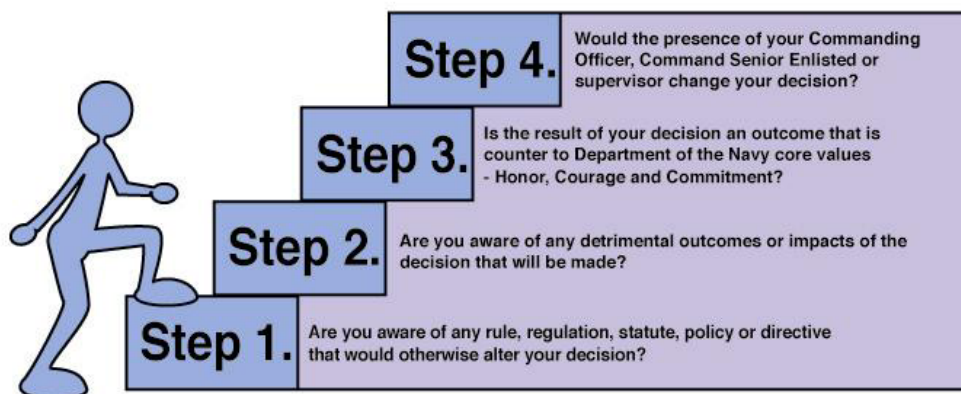
Four Influences on the Decision Maker



Don't be influenced to make unethical decisions.

Figure 12. iTechs Decision Making Awareness Poster

Four Steps Toward the Right Decision



By applying these steps the decision maker will be able to choose an alternative that will result in the best possible outcome.

Don't be influenced to make unethical decisions.

Figure 13. iTechs Decision Steps

Ten Commandments of IT Ethics



1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

Don't be influenced to make unethical decisions.

(The 10 Commandments were developed by the Computer Ethics Institute)

Figure 14. iTechs 10 Commandments



Four Influences on the Decision Maker

Figure 15. iTechs Screen Saver/Wallpaper

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. National Telecommunications and Information Administration Report: *A Nation Online: How Americans Are Expanding Their Use Of The Internet*. February 2002
<http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf>
2. Johnson, Deborah G. *Computer Ethics* 3rd Edition. Upper Saddle River, NJ. Prentice Hall, 2001.
3. The Golden Rule. <http://theosophy.org/tlodocs/GoldnRul.htm>
4. The Golden Rule. <http://www.fragrant.demon.co.uk/golden.html>
5. Michael Josephson (edited by Wes Hanson), *Making Ethical Decisions (4th ed.)*, Marina del Rey, CA: Josephson Institute of Ethics, 1997.
<http://thejosephsoninstitute.org/>
6. Spinello, Richard A. *Case Studies in Information and Computer Ethics*. Upper Saddle River, NJ. Prentice Hall, 1997
7. Moor, James H. *What is Computer Ethics*, found in Spinello, *Case Studies in Information and Computer Ethics*, p.18. This article first appeared in Terrell Ward Bynum, ed., *Computers & Ethics*, Blackwell, 1985, pp.266-75. (A special issue of the journal *Metaphilosophy*.)
8. Websense Inc. Press Release, San Diego, October 30, 2001
<http://www.websense.com/company/news/pr/01/103001.cfm>
9. Websense Inc., News Article "What the Internet means to anyone who wants to stay employed." <http://www.websense.com/company/news/features/01/091201.cfm>
10. Websense Inc, News Room Statistics,
<http://www.websense.com/company/news/stats.cfm>
11. Internal Revenue Service, Criminal Investigation, <http://www.treas.gov/irs/ci/>
12. Bynum, Terrell Ward, "*Ethics and the Information Revolution*." (2000) Reprinted in Spinello, Richard A. and Tavani, Herman T. *Readings in Cyber Ethics*. Sudbury, MA. Jones and Bartlett Publishers, 2001.
13. Deputy Secretary of Defense Memorandum dated 24 Sep 1998
http://www.defenselink.mil/other_info/depsecweb.pdf
14. Joint Ethics Regulation. DoD Directive 5500.7-R. Revised 10 January 2002.
15. GRISWOLD v. CONNECTICUT, No. 496 U.S. Supreme Court. 381 U.S. 479; 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282. March 29-30, 1965, Argued June 7, 1965, Decided
16. Rich, Lloyd L. "*Right To Privacy In The Workplace In The Information Age*." The Publishing Law Center, 1995. www.publaw.com/privacy.html.
17. Roper Center Survey, University of Connecticut. Sponsored by the Freedom Forum. Conducted in November 2000, Questions #38 and #24.
18. "E-mail interception," www.email-policy.com, 2001.
19. Phone interview with Major Greg Gillette, Military Justice Officer, Quantico, Virginia, at 0955 on 16 May 2002.
20. Crane, Joyce. "Is It Healthy to be Stealthy? Using Software to Spy." *The Boston Globe*. 9 Apr 2001, Business Section, pg C2.
21. Gallagher, Mary P., "*FBI Is Upheld in Use of Device That Monitors Keystrokes on Computer*." *New Jersey Law Journal*, 31 December 2001, as found at www.law.com

22. The Associated Press, "Watching Workers' Web Use." Newsday, 10 July 2001, Business and Technology Section, pg. A46.
23. Deibel, Mary. "Labor law covers employee E-mail use." Scripps Howard News Service, *The Patriot Ledger*. 8 May 2000, Business Sec, pg. 27.
24. Gordon, Philip L. "Judge leads fight for workplace privacy" *The Denver Post*. 20 Sept 2001, pg. B-07.
25. "copyright". *Encyclopedia Britannica*.
<http://search.britannica.com/eb/article?eu=26641>. Accessed May 16, 2002.
26. Association of Research Libraries, Washington, D.C., "Timeline: A History of Copyright in the U.S." <http://www.arl.org/info/frn/copy/timeline.html>.
27. McFarland, Michael C., SJ. "Intellectual Property, Information, and the Common Good." (1999) Reprinted in Spinello, Richard A. and Tavani, Herman T. *Readings in Cyber Ethics*. Sudbury, MA. Jones and Bartlett Publishers, 2001.
28. Academic Integrity Committee 1999-2000 cases, Syracuse University,
http://sominfo.syr.edu/students/ai_summ9900cases.html
29. Handbook for Faculty and Academic Administrators, Section III: Procedures Regarding Misconduct in Research, University of Pennsylvania.
http://www.upenn.edu/assoc-provost/handbook/iii_c.html
30. The UT System Crash Course in Copyright,
<http://www.utsystem.edu/OGC/IntellectualProperty/whowns.htm>. 2001
31. Garfinkel, Simson. *Database Nation. The Death of Privacy in the 21st Century*. Sebastopol, CA, O'Reilly & Associates, 2000.
32. Congressional Universe Search, Congressional Bills, keywords Privacy and Policy, May 2002, Lexis-Nexis.
33. <http://www.consumer.gov/idtheft/>. A website maintained by the Federal Trade Commission.
34. "Reports of identity theft still rising." Institute of Management and Administration, New York, January 2002
35. Richtel, Matt. "Credit Card Theft Thrives Online as a Global Market." *New York Times* 13 May 2002
36. Voter Information, League of Women Voters.
http://www.lww.org/voter/govote/taftv_registrationqa.html
37. NAVSO P-3050, Navy Pay and Personnel Manual (PAYPERSMAN)
38. MCO P5000.14C, Marine Corps Admin Procedures Manual (MCAP)
39. MCO P5211.2, Privacy Act of 1974
40. "Virus Creator gets 20 months", eWeek, News and Analysis Section, 6 May 2002
41. McConnell International. "Cyber Crime...and Punishment? Archaic Laws Threaten Global Information". 2000.
42. *The Ten Commandments of Computer Ethics*. Computer Ethics Institute, 1992
43. Government and Personnel Directories, Carroll Publishing Online, 2002
<http://subscribers.carrollpub.com/Subscribers/startpage.asp>
44. Wexley, Kenneth N. and Latham, Gary P. *Developing and Training Human Resources in Organizations (2nd Ed.)*. New York, NY. Harpers Collins, 1991.
45. Goldstein, Irwin L. and Ford, Kevin J. *Training in Organizations (4th Ed.)*. Wadsworth, 2002.

46. Ivancevich, John M., et al. *Management Quality and Competitiveness* (2nd Ed.). Chicago, IL. Irwin Book Team, 1997.
47. Daft, Richard L. *Management* (3rd Ed.). Orlando, FL. Dryden Press, 1994.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Commander, Naval Security Group Command
Naval Security Group Headquarters
Fort Meade, Maryland
4. Ms. Louise Davidson, N643
Arlington, Virginia
5. Ms. Elaine S. Cassara, Branch Head, Information Assurance Branch, C4I
Headquarters, Marine Corps
Washington, DC
6. Mr. William Dawson
Community CIO Office
Washington, DC
7. Ms. Deborah Phillips, Community Management Staff
Community CIO Office
Washington, DC
8. Captain Robert A. Zellman
CNO N6
Arlington, Virginia
9. Dr. Ralph Wachter
Office of Naval Research
Arlington, Virginia
10. Mr. Richard Hale
Defense Information Systems Agency
Falls Church, Virginia
11. Dr. Cynthia E. Irvine, Computer Science Department, Code CS/IC
Naval Postgraduate School
Monterey, California

12. Dr. Floyd Brock, Information Systems Technology, Code IS
Naval Postgraduate School
Monterey, California
13. Deborah Shifflett, Computer Science Department, Code CS
Naval Postgraduate School
Monterey, California
14. Frank Barrett, Graduate School of Business and Public Policy, Code SM
Naval Postgraduate School
Monterey, California
15. LtCol Daniel Barber, USMC
Naval Postgraduate School
Monterey, California
16. Director, Training and Education, MCCDC, Code C46
Quantico, Virginia
17. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia
18. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California
19. Captain Nicolas Yamodis, MC, USN
Naval Medical Information Management Center
Bethesda, Maryland
20. Captain Sidney D. Rodgers, MSC, USN
Naval Medical Information Management Center
Bethesda, Maryland
21. Captain L. J. Walters, MSC, USN, FACHE
Naval Healthcare Support Office, Naval Air Station
Jacksonville, Florida
22. Colonel Terry Ebbert, USMC (Ret)
New Orleans, Louisiana
23. Lieutenant Colonel David F. Bonwit, USMC (Ret)
Madison, Alabama
24. Ms. Elodia M. Blanco
New Orleans, Louisiana

25. Mr. Jasper W. Senter Jr.
Atlanta, Georgia
26. Morris Reece
Meridian, Mississippi
27. Major Jasper W Senter III
Monterey, California
28. Lieutenant Cayetano S. Thornton
Yokosuka, Japan
29. D. C. Boger, Information Systems Department, Code IS
Naval Postgraduate School
Monterey, California